Ballard Spahr LLP

Morris James LLP
ATTORNEYS AT LAW

Trouble: Game Planning for Cyber Incidents:
Practicing & Executing Effective Cyber Incident Response

October 24, 2017

Carl N. Kunz III
Partner
Morris James LLP
Wilmington, Delaware
302-888-6811
ckunz@morrisjames.com

Edward J. McAndrew
Partner & Co-Chair
Ballard Spahr LLP
Privacy and Data Security Group
Wilmington & Washington, D.C.
302-252-4451
mcandrewe@ballardspahr.com

Jeffrey A. Reising
Special Agent
Federal Bureau of Investigation
Baltimore Cyber Task Force
Wilmington Resident Agency
302-357-0174 (Cellular)
302-594-4301 (Office)
jareising@fbi.gov

The New Reality

Ballard Spahr LLP

Navigating Disparate Roles

- Crime Victim
- Target of Government/Regulatory Inquiry/Enforcement
- Civil Litigant
- Subject of Media Scrutiny
- Repeat Customer with a Track Record

Incident Response Scenarios

- Economic & Industrial Espionage
- Theft of IDs, IP, & Other Confidential Data
- System/Device Disruption & Destruction
- Extortion, Stalking and Threats
- Cyber-facilitated fraud/corruption
- Cyber-facilitated Violence

Global Cost of Cybercrime - 2017

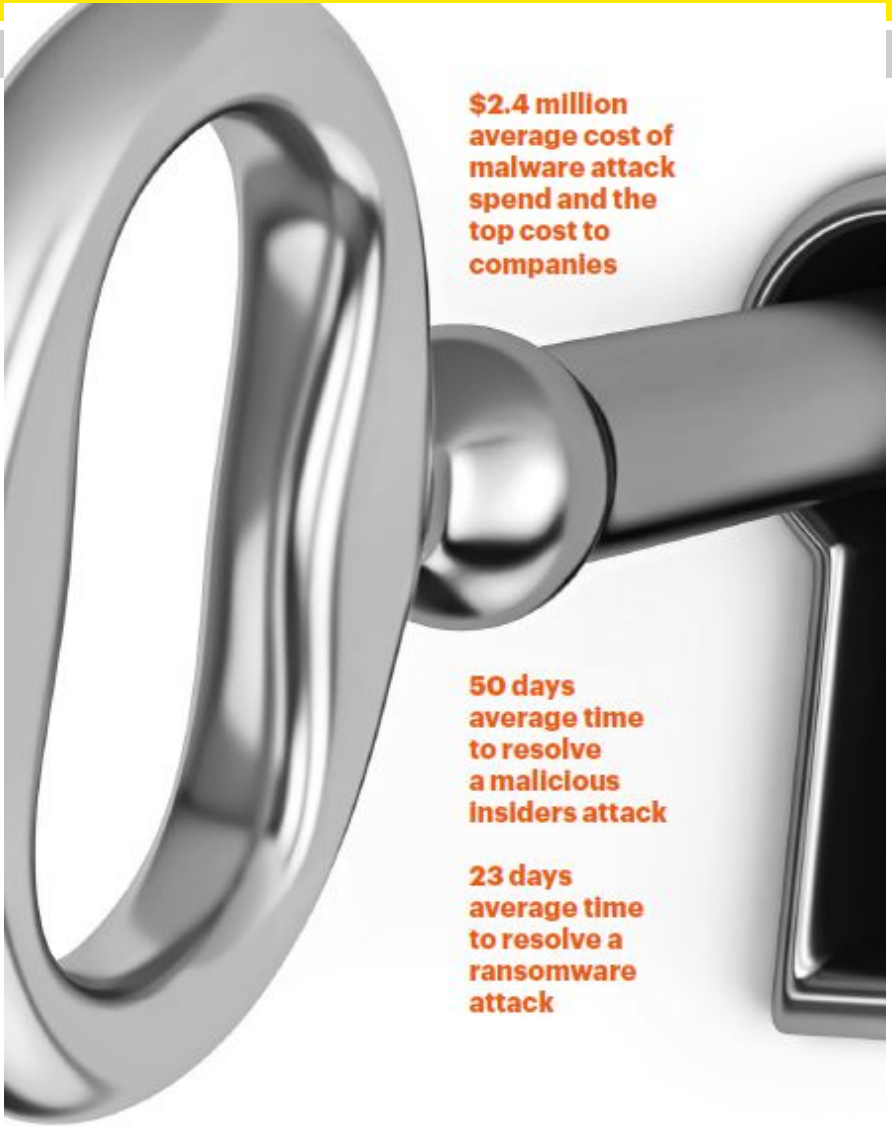
EXECUTIVE SUMMARY

Average annualized cost of cybersecurity (USD) **$11.7M**

Percentage increase in cost of cybersecurity in a year **22.7%**

Average number of security breaches each year **130**

Percentage increase in average annual number of security breaches **27.4%**



$2.4 million average cost of malware attack spend and the top cost to companies

50 days average time to resolve a malicious insiders attack

23 days average time to resolve a ransomware attack

21 SEP 2017 NEWS

FedEx: NotPetya Cost Us $300 Million

BIGLAW, TECHNOLOGY

Global Biglaw Firm 'Paralyzed' By New Ransomware Attack

Uh-oh. What happened to this firm's cybersecurity expertise?

By STACI ZARETSKY

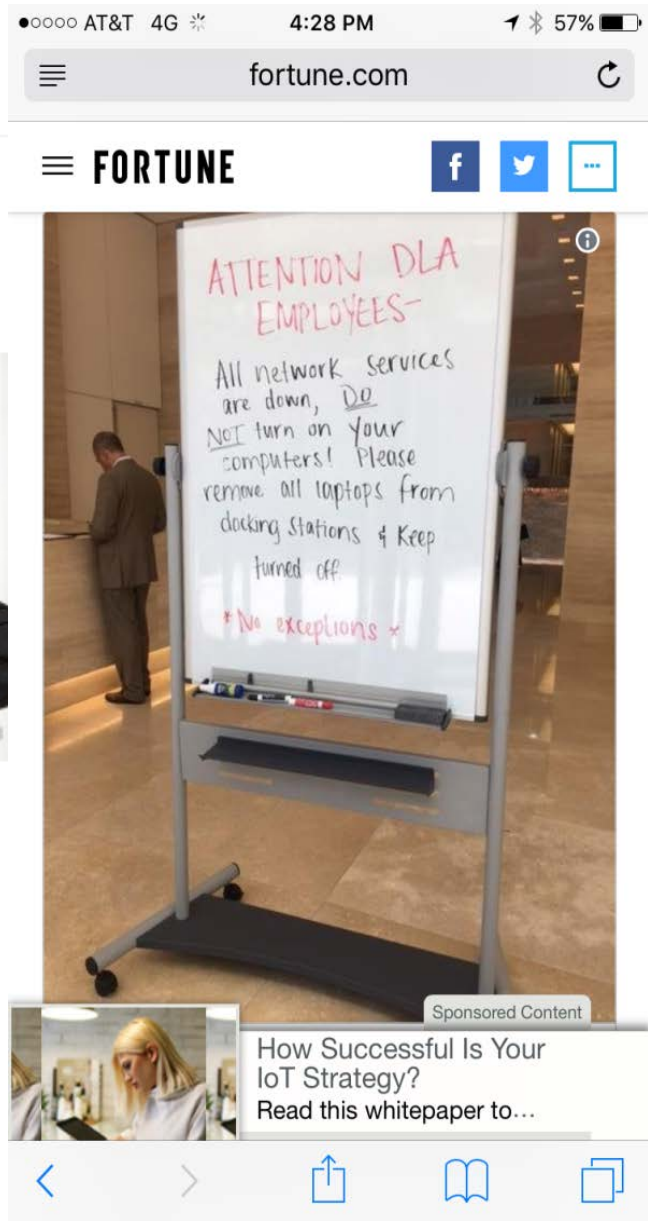
Jun 27, 2017 at 11:14 AM

712 SHARES

In May, the WannaCry ransomware attack infected hundreds of thousands of computers worldwide, and global Biglaw firms like DLA Piper were quick to tout their expertise in cybersecurity compliance, offering solutions for affected companies up to and including crisis management teams and even a 24/7 Rapid Response hotline. Today, it looks like the lawyers at DLA may have to dial their own number, because the firm was just hit by another quickly spreading ransomware attack called Petrwrap/Petya.

Here's the message that was displayed across computer monitors at DLA Piper:

Ballard Spahr LLP



Ransomware Avalanche Hits Prosecutors

2

Hackers hit district attorney's office in Pa., force ransom payment for files

32 shares

MOST READ

Man found dead along Susquehanna River was wearing 'unique' brand of jeans

Ex-state trooper gets prison term for kicking handcuffed Harrisburg activist in the face

Another victim was the Allegheny County District Attorney's Office, which attorney Song initially declined to identify, but which was later outed by the AP. Song said the office paid a $1,400 Bitcoin ransom to free up computer files which had been accessed and locked by hackers using the Avalanche network. The nature of those files was not immediately clear, and an after-hours attempt to reach the DA for comment on Monday was immediately unsuccessful.

The Hackers & the Lawyers

- US v. Hong (SDNY)
- 7 Victim Law Firms
- Hong arrested in Hong Kong
- Hacking over 20-month period
- Spears & Social Engineering
- Over 10 transactions
- Over $4MM in illicit profits
- Theft of IP from 2 Robotics Companies

Chinese Nationals Charged With Hacking Firms to Steal M&A Info

Mark Hamblett, The Am Law Daily
December 27, 2016 | 0 Comments

SHARE
PRINT
REPRINTS

U.S. Attorney for the Southern District Preet Bharara.
Photo: Rick Kopstein/ALM

Updated 12/27/16, 1:20 p.m.

Three Chinese nationals face federal charges for allegedly hacking into two major U.S. law firms in a scheme to trade on information about imminent mergers and acquisitions.

U.S. Attorney Preet Bharara of the Southern District of New York announced Tuesday that Iat Hong, Bo Zheng and Hung Chin have been charged with infiltrating the servers of two law firms in 2014 and 2015 and accessing nonpublic information about pending deals. According to Bharara's office, the information was used in trades that reaped roughly $4 million in illegal profits.

The indictment unsealed Tuesday does not name the law firms, which are referred to as Law Firm 1 and Law Firm 2. According to the charges, Law Firm 1 advised Intel Corp. on its 2015 acquisition of Altera Corp. for $16.7 billion and represented a company that was in deal talks with InterMune Inc., which sold to Roche AG in 2014 for $8.9 billion.

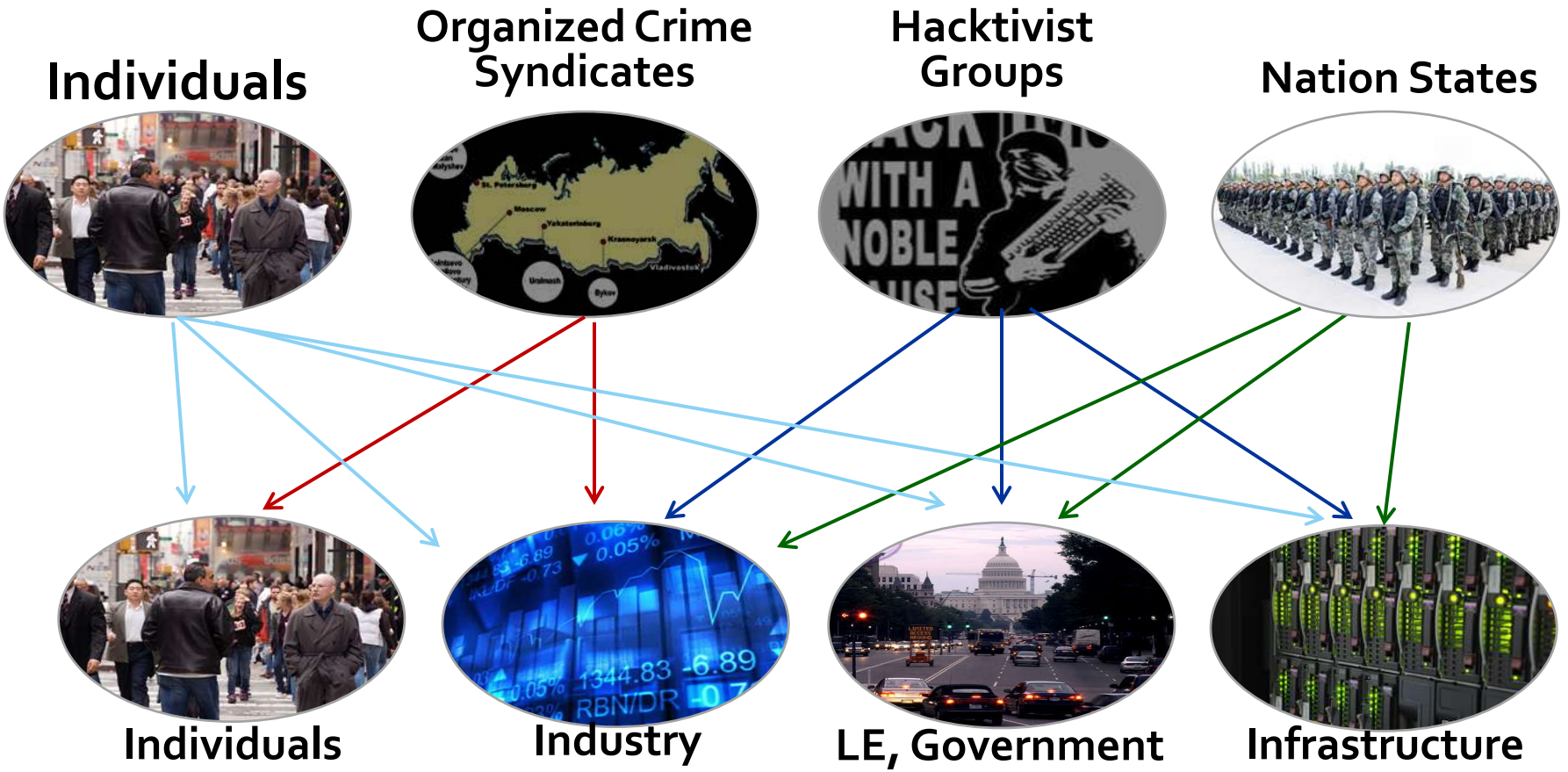
The second major law firm advised Pitney Bowes Inc. in the 2015 acquisition of New York-based e-commerce company Borderfree, the indictment states.

Business Email Compromises

Business E-Mail Compromise
An Emerging Global Threat

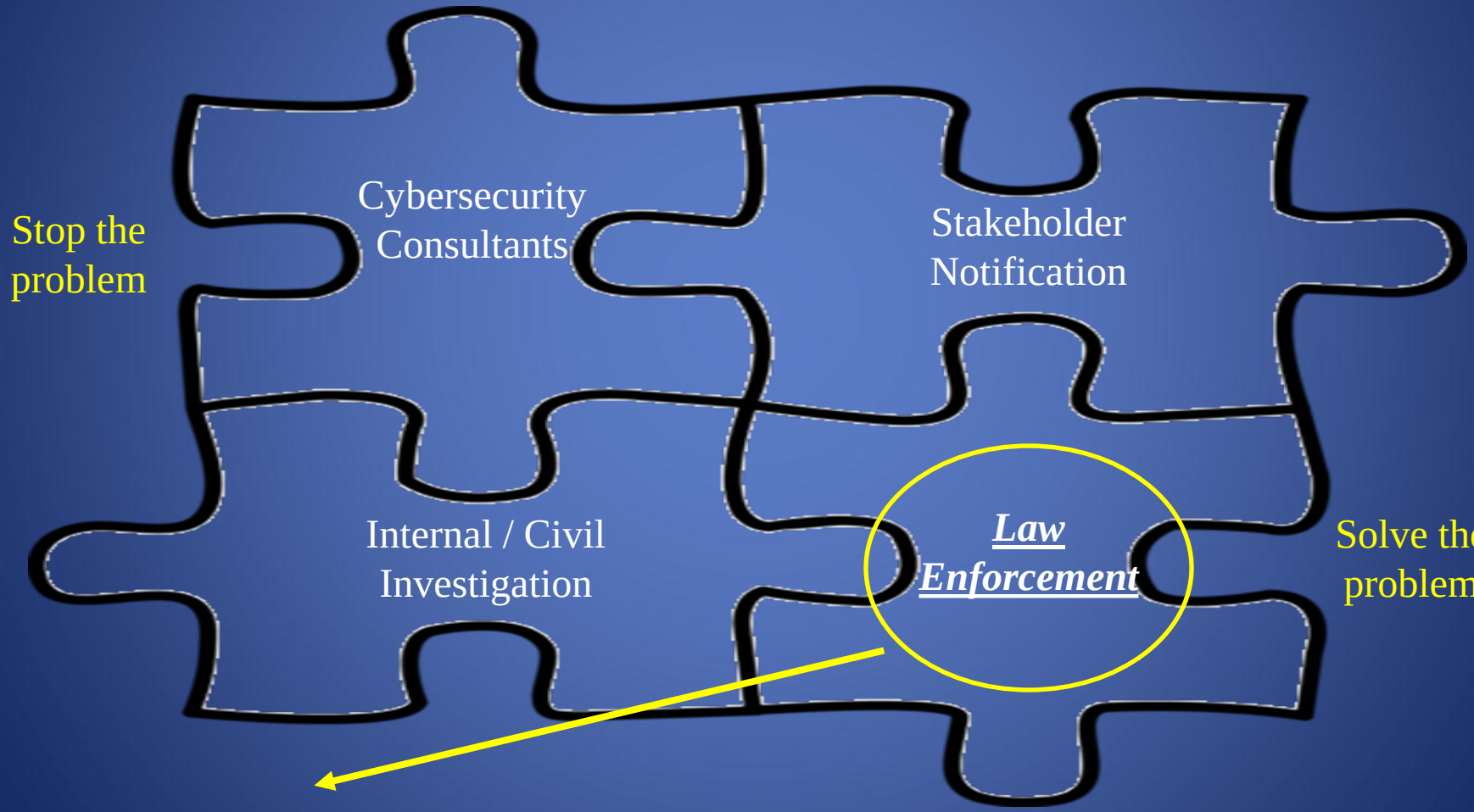
08/28/15

The Bad Guys & The Victims



Ballard Spahr LLP

"We've been hacked…"



Goal: You know who, when and why to call Law Enforcement, and what to expect from us.

Four Take Away Points

1. Local attorneys with global resources
2. Our tools are different from your tools
3. We respect victims' interests
4. You can help us help you

Who we are

Local Attorneys

- 70 attorneys, 3 offices in Colorado
- 5 Computer Hacking & IP Specialists (CHIPs)

National Network

- Computer Crimes & IP Section in DC
  - 40 attorneys + the National Cybercrime Lab
- 270 CHIPs & 94 National Security Cyber Specialists in the USA

Global Resources

- 24/7 High Tech Crime Network
- Bilateral Cybercrime Working Groups
- Mutual Legal Assistance Treaties
- Legal Attachés & IP Law Enforcement Coordinators

Who we are


DEPARTMENT OF THE TREASURY
SPECIAL AGENT
CENTRAL INTELLIGENCE AGENCY
UNITED STATES MARSHAL
US
SPECIAL AGENT
U.S. CUSTOMS PATROL OFFICER
THE DEPARTMENT OF THE TREASURY
SPECIAL AGENT
POLICE
FOREST SERVICE
BORDER PATROL

Cyber Incident Best Practices

Step 1: Prevention and Planning

- Identify "crown jewels"
  - NIST
  - www.nist.gov
- Technology and services in place?
  - Off-site back-up
  - Intrusion capabilities
  - Data loss prevention
  - Authorization for monitoring (banners)
  - Qualified (cyber-savvy) legal counsel
- Have a plan and practice it
  - Cyber incident response team
  - Prioritization of protection
  - Plan to preserve data (good logging capabilities)
  - Plan to notify law enforcement and victims
- Engage with law enforcement
  - Infraguard
  - FBI Cyber task forces
  - USSS Electronic Crimes Task Force

http://www.justice.gov/criminal/cybercrime/

USDOJ: CRM: Computer Cri...

File Edit View Favorites Tools Help

www.cybercrime.gov

THE COMMON LAW IS THE WILL OF *Mankind* ISSUING FROM THE *Life* OF THE *People*

THE UNITED STATES DEPARTMENT of JUSTICE

SEARCH THE SITE

SEARCH

HOME ABOUT AGENCIES BUSINESS RESOURCES NEWS CAREERS CONTACT

Home » Agencies » Criminal Division » Organizations » Computer Crime & Intellectual Property Section

Printer Friendly

Computer Crime & Intellectual Property Section

- About CCIPS
- Press Releases
- Documents and Reports
- Career Opportunities
- Report Crime
- Contact CCIPS
- Criminal Division Home

COMPUTER CRIME & INTELLECTUAL PROPERTY SECTION

ABOUT THE COMPUTER CRIME & INTELLECTUAL PROPERTY SECTION

The Computer Crime and Intellectual Property Section (CCIPS) is responsible for implementing the Department's national strategies in combating computer and intellectual property crimes worldwide. CCIPS prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts. Section attorneys work to improve the domestic and international infrastructure-legal, technological, and operational-to pursue network criminals most effectively. The Section's enforcement responsibilities against intellectual property crimes are similarly multi-faceted. Intellectual Property (IP) has become one of the principal U.S. economic engines, and the nation is a target of choice for thieves of material protected by copyright, trademark, or trade-secret designation. In pursuing all these goals, CCIPS attorneys regularly run complex investigations, resolve unique legal and investigative issues raised by emerging computer and telecommunications technologies; litigate cases; provide litigation support to other prosecutors; train federal, state, and local law enforcement personnel; comment on and propose legislation; and initiate and participate in international efforts to combat computer and intellectual property crime.

GENERAL INFORMATION
COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION

LEADERSHIP

John Lynch
Chief, Computer Crime & Intellectual Property Section

CONTACT

Department of Justice Main switchboard
(202) 514-2000

STAY CONNECTED

Sign up for E-Mail Updates
Subscribe to News Feeds

Facebook Twitter YouTube

U.S. DEPARTMENT of JUSTICE | 950 Pennsylvania Avenue, NW, Washington, DC 20530-0001

ABOUT
The Attorney General
Budget & Performance
Strategic Plans

AGENCIES

BUSINESS & GRANTS
Business Opportunities
Small & Disadvantaged Business
Grants

RESOURCES
Forms
Publications
Case Highlights
Legislative Histories

NEWS
Justice News
The Justice Blog
Public Schedule
Videos
Photo Gallery

CAREERS
Legal Careers
Interns, Recent Graduates, and Fellows
Diversity Policy
Veteran Recruitment

CONTACT

JUSTICE.GOV

Site Map
A to Z Index
Archive
Accessibility
FOIA
No FEAR Act
Information Quality
Privacy Policy
Legal Policies & Disclaimers

For Employees
Office of the Inspector General
Government Resources
USA.gov
BusinessUSA

Understanding the Cyber Incident

- Type of attack
- Means of Access
- Data Subject to Exposure
- Movements within Networks
- Data compromise
- Time Period of Incident
- Current Status of Networks and Devices
- Mitigation and Remediation

Cyber Incident Best Practices

Step 2: Make an Assessment

- Identify and preserve:
  - intrusion vs. glitch
  - Affected computer(s)
  - Origin
  - Malware
  - Exfiltration
  - Who is currently logged in
  - Current connections
  - Running processes
  - Open ports, apps
  - Any communications

Step 3: Minimize Damage

- Restore to back ups?
- Reroute or block traffic
- Contact exfil location
- Null routing
- Closing ports

Cyber Incident Best Practices

Step 4: Document steps and Record Information

- Document all investigative steps
- Image the affected computer (Consent to Search Form)
- Keep Logs, Notes and Data
  - Preserve all relevant logs
  - Note all response steps taken
  - Note all relevant events
  - Note who responded, and how much time ($) they spent

Step 5: Notify

- FBI
- Secret Service
- Homeland Security
  - National Cybersecurity & Communications Integration Center

Cybersecurity Unit
Computer Crime & Intellectual Property Section
Criminal Division
U.S. Department of Justice

1301 New York Avenue, N.W., 6th Floor, Washington, D.C. 20530 - CYBERSECURITY.CCIPS@USDOJ.GOV - (202)514-1026

Best Practices for Victim Response and Reporting of Cyber Incidents

Version 1.0 (April 2015)

Any Internet-connected organization can fall prey to a disruptive network intrusion or costly cyber attack. A quick, effective response to cyber incidents can prove critical to minimizing the resulting harm and expediting recovery. The best time to plan such a response is now, *before* an incident occurs.

This "best practices" document was drafted by the Cybersecurity Unit to assist organizations in preparing a cyber incident response plan and, more generally, in preparing to respond to a cyber incident. It reflects lessons learned by federal prosecutors while handling cyber investigations and prosecutions, including information about how cyber criminals' tactics and tradecraft can thwart recovery. It also incorporates input from private sector companies that have managed cyber incidents. It was drafted with smaller, less well-resourced organizations in mind; however, even larger organizations with more experience in handling cyber incidents may benefit from it.

Cyber Incident Best Practices

Steps 6: Victim Response

- Best practices for victim response and reporting of cyber incidents (April, 2015)
  - https://www.justice.gov/criminal-ccips/cybersecurity-unit
- Other potential victims
  - 48 states have passed database breach notification laws
  - But delayed notice is allowed if it impedes an investigation

Cyber Incident Best Practices

What not to do:

- Do not use compromised system to communicate
- Do not hack or damage another network

After an incident:

- Remain vigilant
- Initiate new protection measures
- After-action reports

RANSOMWARE

- Prevention
  - Social engineering/phishing
  - Centralized patching system
- If infected:
  - Isolate
  - Secure backup data by taking offline
  - Change passwords
- Report to Law Enforcement

When to Call Law Enforcement

Thresholds

- Is there Federal jurisdiction & venue?
- What is the scale of victimization?
  - Number of victims
  - Financial loss

- What is the Federal interest involved?
  - Type of entity victimized
  - National Security, Health & Infrastructure, Economic Security
- What civil remedies are available?

Governmental Concerns

- Severity of Attack
- Organizational Resiliency
- Impact on Industry Sectors
- Economic and National Security Implications
- Pervasiveness and Connectedness of Incident(s)
- Attribution
- Evidence Gathering and Victim Cooperation
- Potential for Success of Different Governmental Tools

When to Call Law Enforcement

Common Federal Cybercrimes

- Any unauthorized access (hack) into –
  - Networks, servers, computers, routers, ATMs, POS devices...
  - Online accounts
- Installation of malware, including ransomware
- Denial of service attacks
- Insider and former employee trade secret theft
- Business Email Compromise / phishing / ACH fraud
- Defacing or spoofing a website
- Internet-related identity theft

Why Call Law Enforcement?

Regulators

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

U.S. SECURITIES AND EXCHANGE COMMISSION · MCMXXXIV

U.S. Department of Health & Human Services

cfpb Consumer Financial Protection Bureau

FCC Federal Communications Commission

Why Call Law Enforcement?

Stockholders

SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior To Breach

Could Yahoo be in trouble with the SEC?

By Hayley Tsukayama September 28

THE WALL STREET JOURNAL.

By **TATYANA SHUMSKY**

Sept. 19, 2016 5:31 p.m. ET

The SEC has yet to bring a case against a company that failed to disclose a cyberincident, but officials haven't ruled out doing so. "Can I envision circumstances where we would bring an action? Sure," said Stephanie Avakian, the SEC's deputy director of enforcement, at a February conference. "But it would have to be a significant disclosure failure to warrant that."

Why Call Law Enforcement?

Public Relations

Lawmakers grill former Equifax chairman over data breach

By KEVIN FREKING, ASSOCIATED PRESS ·
WASHINGTON — Oct 3, 2017, 3:47 PM ET

Share with Facebook | Share with Twitter

ormer chairman and CEO of Equifax Richard F. Smith testifies before the Digital Commerce and Consumer Protection Subcommittee of the House Commerce Co… more

House Republicans and Democrats on Tuesday grilled Equifax's former chief executive over the massive data hack of the personal information of 145 million Americans, calling the company's response inadequate as consumers struggle to deal with the breach.

The New York Times

BUSINESS DAY

S.E.C. Says It Was a Victim of Computer Hacking Last Year

By ALEXANDRA STEVENSON and CARLOS TEJADA SEPT. 20, 2017

SEC Says It Told U.S. Security Officials of Hack Months Ago

Former Equifax CEO says breach boiled down to one person not doing their job

Why Call us?

State Laws

Montana and Washington State Propose Amendments to Data Breach Legislation

Two Wyoming Bills Amending the State's Breach Notification Statute Are Headed to the Governor

Posted on February 27, 2015

Kentucky Enacts Data Breach Notification Law

California Bulks Up Security Breach Notification Requirements

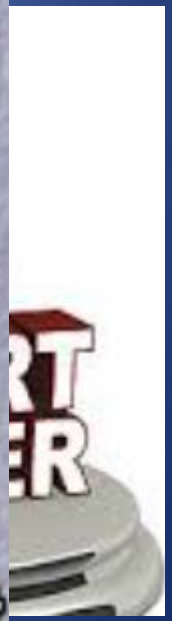
Colorado	Colo. Rev. Stat. § 6-1-716

Why Call Us

Our tools are different…

Why Call Us

Our tools are different…



Our Best Investigative Tools

Law Enforcement Remedial Tools

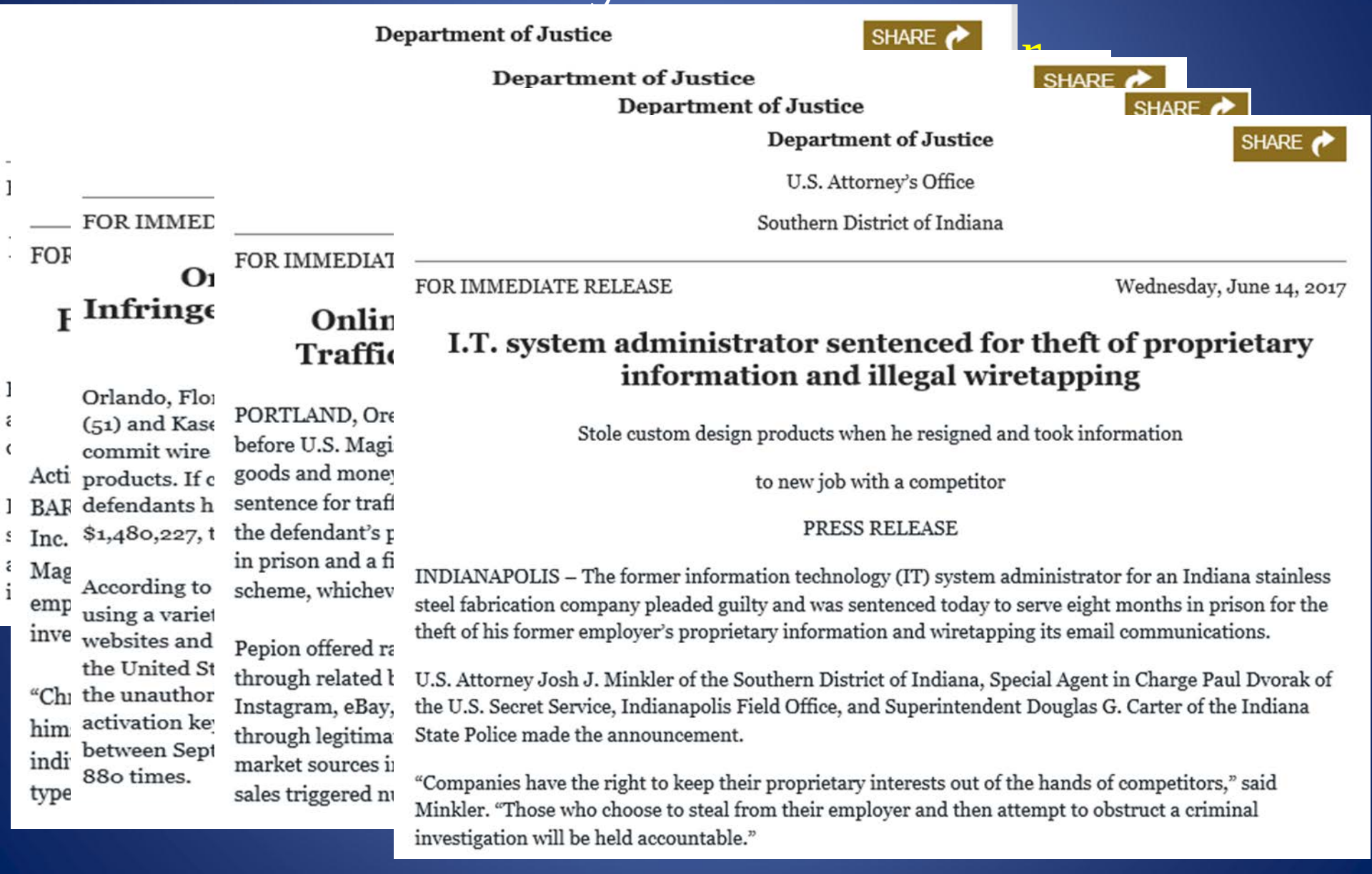
Title 18 United States Code

- ID Theft (§ 1028): 5-15 years
- Access Device Fraud (§ 1029): 10-15 years
- Computer Fraud and Abuse (§ 1030): 5-10 years
- Wire Fraud (§ 1343): 20 years
- Economic Espionage (§ 1831):
  - Individual – 15 years and $5M
  - Entity – $10M or 3x value of the stolen trade secret
- Theft of Trade Secrets (§ 1832): 10 years
  - Individual – 10 years
  - Entity – $5M or 3x value of the stolen trade secret
- Interception of Communications (§ 2511): 5 years

Law Enforcement Remedial Tools

- Mandatory Victim's Restitution Act (§ 3663A)
  - A judgment that is non-dischargeable
  - Calculated without regard to a defendant's ability to pay
- Financial Fraud Kill Chain
  - Claw back international wire transfers > $50,000
  - Notification required within 72 hours of transfer

Why Call Us



Department of Justice

SHARE

Department of Justice

SHARE

Department of Justice

SHARE

Department of Justice

SHARE

U.S. Attorney's Office

Southern District of Indiana

FOR IMMEDIATE RELEASE

Wednesday, June 14, 2017

I.T. system administrator sentenced for theft of proprietary information and illegal wiretapping

Stole custom design products when he resigned and took information

to new job with a competitor

PRESS RELEASE

INDIANAPOLIS – The former information technology (IT) system administrator for an Indiana stainless steel fabrication company pleaded guilty and was sentenced today to serve eight months in prison for the theft of his former employer's proprietary information and wiretapping its email communications.

U.S. Attorney Josh J. Minkler of the Southern District of Indiana, Special Agent in Charge Paul Dvorak of the U.S. Secret Service, Indianapolis Field Office, and Superintendent Douglas G. Carter of the Indiana State Police made the announcement.

"Companies have the right to keep their proprietary interests out of the hands of competitors," said Minkler. "Those who choose to steal from their employer and then attempt to obstruct a criminal investigation will be held accountable."

FOR IMMEDIAT

Onlin
Traffi

PORTLAND, Ore
before U.S. Magi
goods and money
sentence for traff
the defendant's p
in prison and a fi
scheme, whichev

Pepion offered ra
through related b
Instagram, eBay,
through legitima
market sources i
sales triggered nu

FOR IMMED

Infringe

Orlando, Flor
(51) and Kase
commit wire
products. If c
defendants h
$1,480,227, t

According to
using a variet
websites and
the United St
the unauthor
activation ke
between Sept
880 times.

US v. Blake Snowden

Former Employee Hacking / Trade Secret Theft

Arvada Man Sentenced To 30 Months In Federal Prison For Hacking Into Computer System Of His Former Employer

DENVER – Blake Douglas Snowden, age 44, of Arvada, Colorado, was sentenced yesterday by U.S. District Court Judge Christine M. Arguello to serve 30 months in federal prison, followed by 3 years of supervised release for unauthorized access to a protected computer and unauthorized interception of an electronic communication, the U.S. Attorney's Office and the Federal Bureau of Investigation (FBI) announced. Snowden was also ordered to pay restitution of $25,354 to [redacted] Inc., his former employer and the company whose computer and email he hacked. Judge Arguello found that the total loss Snowden caused to [redacted] was $1,697,471.76. The defendant, who appeared at the sentencing hearing free on bond, was ordered to report to a Bureau of Prisons facility within 30 days of designation.

Snowden, no relation to the infamous Edward Snowden, was indicted by a federal grand jury in Denver on November 20, 2013. He pled guilty before Judge Arguello on May 28, 2014. He was sentenced on March 12, 2015. The issue regarding loss took substantial time to resolve, explaining t[redacted]n

US v. Andrianakis et al.

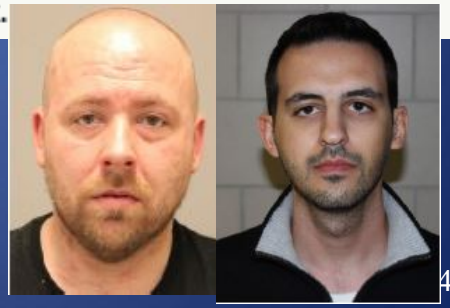
Hacking Customers / Password Theft

Two Men Who Breached [redacted].com Indicted and Arrested on Conspiracy and Fraud Related Charges

Two men have been arrested after breaching the computer services of Colorado based [redacted] a company that operates a[redacted] website, announced U.S. Attorney John Walsh for the District of Colorado and Special Agent in Charge Thomas Ravenelle for the Denver Division of the Federal Bureau of Investigations (FBI). Brandon Bourret, 39, of Colorado Springs, Colorado and Athanasios Andrianakis, 26, of Sunnyvale, California, were arrested today without incident at their homes. Both made initial appearances today, where they were advised of their rights and the charges pending against them.

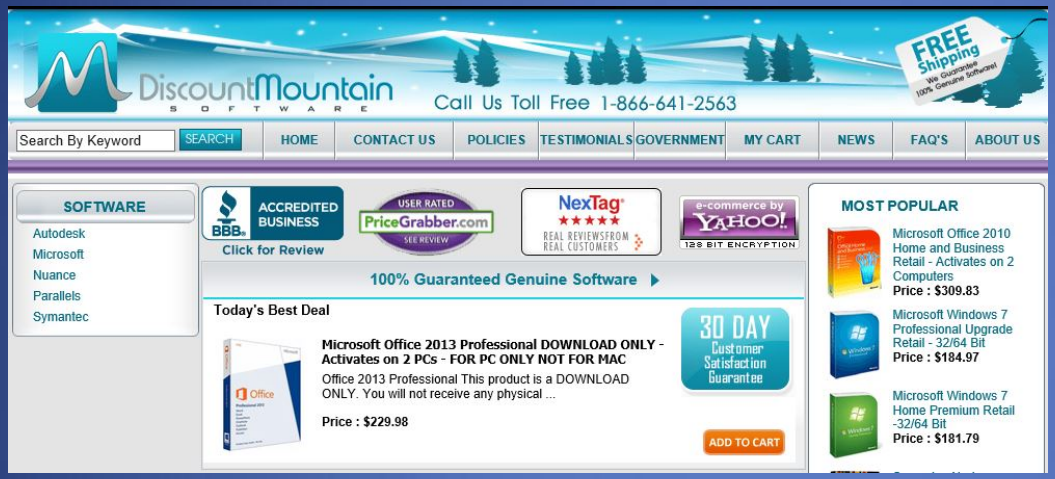
According to the indictment, beginning on July 12, 2012 and continuing through July 1, 2014, Bourret and Andrianakis knowingly conspired to commit acts and offenses against the United States, namely computer fraud and abuse, access device fraud, identification document fraud and wire fraud. The indictment further alleges that there was interdependence among the members of the conspiracy.

The purpose of the conspiracy was for the conspirators to enrich themselves by selling passwords and unauthorized access to private and password protected information, images and videos on the Internet and by selling private and password protected information, images and videos that the conspirators obtained from the Internet.



US v. Lockwood et al.

Software Key Theft / Insufficient Civil Remedies



US District Court Civil Docket

U.S. District - Colorado
(Denver)

1:13cv1699

Microsoft Corporation v. Discount Mountain, Inc. et al

This case was retrieved from the court on Tuesday, April 15, 2014

Date Filed:	06/27/2013		
Assigned To:	Judge Richard P. Matsch	Class Code:	OPEN
Referred To:		Closed:	
Nature of suit:	Copyrights (820)	Statute:	17:501
Cause:	Copyright Infringement	Jury Demand:	Defendant
Lead Docket:	None	Demand Amount:	$0
Other Docket:	None	NOS Description:	Copyrights
Jurisdiction:	Federal Question		

US v. Lockwood et al.

Software Key Theft / Insufficient Civil Remedies

DENVER BUSINESS JOURNAL

Denver man charged in $90M software piracy ring

Jun 23, 2015, 7:14am MDT **Updated** Jun 23, 2015, 7:29am MDT

The U.S. Department of Justice brought charges against a Denver man and two others in what it is calling one of the largest software piracy schemes ever prosecuted.

Charges were brought against: Casey Lee Ross, 28, of Kansas City; Reza Davachi, 41, of Damascus, Md.; and Matthew Lockwood, 37, of Denver. Ross and Lockwood entered guilty pleas.

Davachi is also accused of selling $1.24 million worth of key codes to Lockwood, who did business as Discount Mountain Inc. Lockwood also admitted to purchasing $1.13 million worth of key codes from Ross, and another $1.57 million worth from unidentified people in the state of Washington.

Overall, the Justice Department said the alleged fraud reaped $30 million in profits on $90 million in sales of pirated software.

What to Expect from Law Enforcement

First, Do No Harm…

- We prioritize avoiding re-victimization
- We do not disclose non-public information or discuss ongoing investigations
- We work with you to minimize disruption to your client's network and operations

- We have tools to protect sensitive information

What to Expect

- "Best Practices for Victim Response and Reporting of Cyber Incidents" (CCIPS 4/2015)
- "Reporting Intellectual Property Crime: A Guide for Victims of Copyright Infringement, Trademark Counterfeiting, and Trade Secret Theft" (CCIPS 6/2016)
- "Your Secrets Are Safe With Us: How Prosecutors Protect Trade Secrets During Investigation and Prosecution" (American Journal of Trial Advocacy, Vol. 38: 461, 2015)

www.justice.gov/criminal-ccips

What to Expect

The Wheels of Justice Turn Slowly…

- Four Essential Requirements: interviews, forensic images, logs, and **_loss records_**
  - Consent to Search
- You will not get a copy of our reports or seized evidence during the investigation & prosecution
- Victims' Rights
  - Communication and input into key decisions
- Referrals

Involvement in Criminal Litigation

- Witness Testimony
- “Expert” Services
- Managing the Media
- Data Production/Protection in the Litigation Process
- Conviction & Sentencing
- Regulatory/Civil Litigation Spillover

Reporting an Incident

Who to Call:

- Secret Service Cybercrimes
- FBI Field Office Cyber
- Homeland Security Cyber
- U.S. Attorney's Offices
- A.G.'s Offices
- State and Local Law Enforcement

File a Complaint:

- The Internet Crime Complaint Center
  - www.IC3.gov
- The National IP Rights Coordination Center
  - www.iprcenter.gov
- The US Computer Emergency Readiness Team
  - www.us-cert.gov

Reporting an Incident

Infragard Member Alliance – Denver

- A cooperative between the U.S. Government and businesses, academic institutions, and state and local agencies dedicated to securing critical infrastructure

www.infragard.org

Colorado Electronic Crimes Task Force

- A national network private sector, academic, and state and federal law enforcement collaborating to prevent, detect and investigate electronic crimes, including attacks against critical infrastructure and financial payment systems

www.secretservice.gov/investigation/